INTERNATIONAL MARITIME ORGANIZATION

IMO

E

MARITIME SAFETY COMMITTEE
76th session
Agenda item 4

MSC 76/ISWG/5
29 July 2002
Original: ENGLISH

MEASURES TO ENHANCE MARITIME SECURITY

Intersessional Working Group on Maritime Security (ISWG)

International Code for the Security of Ships and of Port Facilities

Consolidated proposed Part B of the International Maritime Security Code

Note by the Chairman

SUMMARY	
Executive summary:	This document provides the consolidated text of proposed Part B of the draft ISPS Code prepared by the Chairman of the ISWG
Action to be taken:	Paragraph 3
Related documents:	MSC 75/24 and MSC 75/WP.18, paragraph 91 and annex 4

1 MSC 75 noted that, due to time constrains, the Working Group on Maritime Security (MSWG) was not able to consider and prepare texts for recommendatory part B of the draft ISPS Code leaving it as set out in annex 3 to document MSC 75/WP.7.

2 In order to assist the ISWG in its work on the development of part B of the ISPS Code, the Chairman has developed appropriate draft text as set out at annex. The text is presented in the order of document MSC 75/WP.18/Add.1, annex 3, which was noted and approved by MSC 75 for review by the ISWG and onward submission to the Maritime Security Conference.

Action requested of the ISWG

3 The ISWG is invited to note the above, consider the attached text and take action as appropriate.

***

ANNEX

Part B

Recommended guidance regarding the provisions of Chapter XI-2 of the Annex to the International Convention for the Safety of Life at Sea, 1974 as amended

1 Introduction

1.1 [*Editorial Note: This introduction may in whole or in part sit better in Part A of the Code or in place of the Preamble*] The risks associated with acts that threaten the security of ships and port facilities have to be addressed by the international maritime community. Those intending to perpetrate such acts may target either the ship or the port facility. The ship itself could be a weapon, or it could be used to transport persons intending to cause a security incident or their equipment. The port facility could also be used as a platform for committing acts giving rise to a security incident. All such activities could lead to death and injury to ship's crews, port workers, passengers, and the wider community. They have to be guarded against.

1.2 This Code establishes an international marine security framework, which applies to ships used in international trade and to the related port facilities. Ship and port facility security is a risk management activity, which must be based on a clear assessment of the risks faced. Recognizing that some disruption will occur as the security level increases, security measures should seek to minimise disruption to normal maritime and port activities.

1.3 Each Contracting Government will need to set the security level applying to its ships and port facilities and ships using its port facilities at any particular time. The Code defines three security levels, 1, 2 and 3 for international use. All ships and port facilities to which the Code applies must have, and maintain, a minimum level of security (security level 1) and must be able to demonstrate that they can respond in an appropriate manner when the security level moves to 2 and, when there is credible information that a security incident is probable or imminent, to Security Level 3.

1.4 Companies operating ships over 500 tonnes on international voyages have to designate Company and Ship Security Officers and have to prepare a Ship Security Plan for each vessel. The Ship Security Plan has to demonstrate the measures applied to maintain security level 1 and the additional actions to be taken when moving to security level 2. The Ship Security Plan also has to show that the ship has arrangements in place which would allow it to move to security level 3 when that level applies though the measures to be taken at security level 3 are likely to be set by the ship's flag State or the administration responsible for the port facility the ship is using. The Ship Security Plan has to be approved by the ship's flag State and it must carry a certificate indicating that it has an approved Ship Security Plan on board. The Plan itself remains protected from unauthorised disclosure. Certain subsequent amendments to an approved Ship Security Plan have to be approved by the ship's flag State.

1.5 The Ship Security Plan certificate will become subject to a Port State Control inspection. Port State Control officers are expected to work with Port Facility Security Officers to ensure all requirements of SOLAS are met including the provisions of this Code. The authority of the Port State Control officer is not pre-empted by any document issued under this Code.

1.6 Following a Port Facility Security Assessment, port facilities to which this Code applies will appoint a Port Facility Security Officer and prepare a Port Facility Security Plan. The Port Facility Security Plan has to demonstrate the measures to maintain security level 1 and the capability to move to security level 2. The Port Facility Security Plan also has to show how the port facility will move to security level 3 when that security level applies. The Port Facility Security Plan has to be approved by the Contracting Government responsible for the port facility and that responsibility should not be delegated.

1.7 This Code contains mandatory provisions and guidance relating to:

.1 security levels;

.2 the appointment, roles and responsibilities of Company and Ship Security Officers;

.3 the preparation, possible content and approval of the Ship Security Plan;

.4 port State control provisions;

.5 port facility security assessments;

.6 the appointment, role and responsibility of the Port Facility Security Officer, and

.7 the preparation, possible content and approval of the Port Facility Security Plan.

1.8 Security measures will on occasion lie uneasily with established safety provisions. Security may involve limiting or barring points of access while safety considerations may dictate maximising the number of possible evacuation routes. A careful balance will need to be struck between safety and security bearing in mind that a common objective of both regimes is the saving of life. As an example, a door that is capable of being opened in one direction only may provide security while also satisfying safety requirements.

1.9 The mandatory requirements of this Code will impose additional responsibilities and burdens on many employed in the shipping and port industries. It is essential that those involved in security, as well as safety, have the resources, manpower and competencies needed to allow them to perform their tasks effectively.

1.10 The purpose of this Code is to deter or detect possible acts that could threaten the security of ships or port facilities. The Code's provisions could necessarily involve control of, or restrictions on, some activities which at other times and locations would be unfettered. Nothing in the Code is intended to restrict internationally accepted individual rights including trade union rights, rights of lawful assembly and the standards applying to maritime workers. However, as with safety, security considerations may demand that a careful balance will need to be struck to protect national security and public welfare.

2 Definitions

No additional guidance.

3 Application

No additional guidance.

4 Responsibility of Contracting Governments

4.1 A Contracting Government may make information on their Port Facility Security Plan or Port Facility Security Assessment available to another Contracting Government to enable verification of their conformity with this Code.

4.2 In designating a Recognized Security Organization (RSO), Contracting Governments should give consideration to the competency of such an Organization. RSO's should be able to demonstrate:

.1 expertise relevant aspects of security, for example, have a background in providing security services in the aviation industry;

.2 experience with ship/port operations;

.3 an appreciation of the likely security risks that could apply during a ship/port interface and how to mitigate those risks;

.4 the ability to undertake and sustain the expertise required with surveyors or personnel properly vetted for trustworthiness; and

in the case of providing security services for ships:

.5 appropriate geographical coverage that may be worldwide if necessary.

4.3 In setting the security level Contracting Governments should take account of general and specific threat information. Administrations should set the security level on their ships at one of three levels; normal (Level 1), enhanced (Level 2) or high (Level 3). Standardisation of these levels on ships will facilitate interaction with port facility security plans. To assist in the harmonisation of these provisions, Contracting Governments should adopt the same system of three security levels for port facilities, even if the threat information is promulgated using a different scale, i.e., 1 to 5. In setting the security level, Contracting Governments should hold Level 3 in reserve for when there is credible information that a security incident is probable or imminent. Therefore, Security Level 3 will equate to very high levels of threat.

4.4 Contracting Governments should consider how information on changes in security levels should be promulgated rapidly to those who need to know. Administrations may wish to use NAVTEX messages or Notices to Mariners as the method for notifying such changes in security levels to ship and ship company security officers. Or, they may wish to consider other methods of communication that provide equivalent or better speed and coverage. Contracting Governments should establish a means of notifying Port Facility Security Officers of changes in security levels. Contracting Governments should compile and maintain the contact details for a list of those who need to be told of changes in security levels. Whereas the Security Level need not be regarded as being particularly sensitive, the underlying threat information may be highly sensitive. Contracting Governments should give careful consideration to the amount of information conveyed and the method by which it is conveyed, to ship, ship company and port facility security officers.

4.5 Contracting Governments should consider carefully the promulgation of information relating to facilities within their jurisdiction which, following a Port Facility Security Assessment, have been determined to meet the provisions of regulation XI-2/6.5 of the Convention. [*Editorial Note: this is a reference to the "exception clause" for ports that only*

occasionally receive ships on international voyages]. Those ports that do not need a plan when the Assessment is first undertaken may need to receive ships requiring security protection from time to time and circumstances may alter so that they do need a plan, possibly at short notice in the future. Similarly, ports that are determined as needing a plan may subsequently no longer need one. It is clearly not desirable for information on whether a port is deemed to need a security plan to be easily available or discernable. It is also undesirable to have a large burden of updating and checking the validity of information on ports across the globe. However, it is necessary for company and ship security officers to know in advance of arrival who should be contacted to liaise on security issues. It is therefore recommended that:

.1 information on which ports have a port facility security plan should be retained centrally by Contracting Governments and not shared widely. It is for the Contracting Government to decide with whom it shares this security information but this information should be protected to maintain the integrity of international shipping and ports; and

.2 Contracting Governments should establish a domestic system in which there is central, regional, or port specific points of contact that cover all ports or a mix of these options that does not identify which of the ports do not have a security plan. These points of contact should be made available widely and should be deposited with the Organisation. Approaching ships who wish to engage in ship port facility activity need only contact the appropriate point to ensure that the destination port is alert to its security status and intended arrival. The central or regional point of contact may be a Port Facility Security Officer (PFSO) or the contact point may establish a link between the ship security officer and the PFSO or, in the case of a port that does not have a security plan (and therefore does not have a PFSO) a person suitably qualified to undertake this role.

4.6 Contracting Governments should provide the contact details of a Government officer to whom ship, company and port facility security officers designated within their jurisdiction and in accordance with this Code can report security concerns. This point of contact should assess such reports before taking appropriate action. Such reported concerns may have a bearing on the security measures falling under the jurisdiction of another Contracting Government. In that case, the Contracting Governments should consider contacting their counterpart in the other Contracting Government to discuss whether remedial action is appropriate. For this purpose, the contact details of the Government officers should be communicated to the Organisation.

4.7 Contracting Governments should establish appropriate measures to enhance the security of fixed and floating platforms to ensure that any security provisions applying to such platforms allow interaction with those applying to ships covered by this Code.[1]

5 Declaration of Security

5.1 The Declaration of Security (DOS) should be completed when the Contracting Government of the port facility deems it to be necessary. Requirements for the DOS should be included in the port facility security plan. The need for a Declaration of Security may be indicated by the results of the Port Facility Security Assessment or the Ship Security Assessment.

1. Refer to Establishment of Appropriate Measures to Enhance the Security of Ships, Port Facilities, and Fixed and Floating Platforms Not Covered by Part B of SOLAS Chapter XI, adopted by the Conference on Maritime Security by resolution [X].

It is likely that a DOS will be used at higher security levels and for ship/port interface activities that pose a higher risk to people, property, or the environment for reasons specific to that ship, including its cargo or passengers, or the circumstances at the port facility, or a combination of these factors. The main purpose of a DOS is to demonstrate the compliance with and identification of clear responsibility for security measures.

5.2 The DOS is an agreement between the Port Facility and the Ship that could be for a single ship/port interface activity or be a standing agreement for recurring and similar ship/port interface activities. Regardless, the time period, security level, and contact information should be specified in the agreement. The DOS should be signed and dated by both the Port Facility and the Ship Security Officer to indicate compliance with this Code. A change in the security level may require that a new or revised DOS be completed.

5.3 The DOS should be completed in a working language common to both the Ship and Port Facility Security Officer.

5.4 When a ship intends to call at a port facility which the Contracting Government has determined meets the provisions of regulation XI-2/6.X of the Convention, a DOS may be drawn-up by a Ship Security Officer in co-operation with a designated local official for the port facility. The Declaration could subsequently be offered to the next port or ports of call as evidence that the security of the ship had not been compromised by calling at a port facility not covered by all of the provisions of this Code.

5.5 Also, when a ship wishes to demonstrate that it has maintained a higher level of security than the level of security prevailing at the port facility, it may choose to initiate a DOS. The DOS could be offered to the ship company or Administration as evidence that the ship has maintained the higher level of security despite the port facility operating at a lower level.

5.6 A port facility security officer may also initiate a DOS prior to ship/port interfaces that are identified in the Port Facility Security Assessment as being of particular concern. Examples may include the embarking or disembarking passengers, and the transfer, loading or unloading of dangerous cargoes. The Assessment may also identify facilities at or near highly populated areas or economically significant operations that warrant a Declaration of Security.

5.7 A model DOS is included in annex 1 to this Part.

6 Obligations of the Company

No additional guidance.

7 Ship Security

Additional guidance on ship security is provided in Section 8 on the Ship Security Assessment and Section 9 on the Ship Security Plan.

8 Ship Security Assessment

Security assessment

8.1 Prior to commencing the ship security assessment, the company security officer [2] should take advantage of information available on the assessment of threat for the ports at which the ship will call or at which passengers embark or disembark and about the port facilities and their protective measures. The company security officer should study previous reports on similar security needs. Where feasible, the company security officer should meet with appropriate persons on the ship and in the port facilities to discuss the purpose and methodology of the assessment.

8.2 The company security officer should obtain and record the information required to conduct an assessment, including:

.1 the general layout of the ship;

.2 the location of areas which should have restricted access, such as bridge, engine-room, radio-room etc.;

.3 the location and function of each actual or potential access point to the ship;

.4 the open deck arrangement including the height of the deck above the water;

.5 the emergency and stand-by equipment available to maintain essential services;

.6 numerical strength, reliability and security duties of the ship's crew;

.7 existing security and safety equipment for protection of passengers and crew;

.8 existing agreements with private security companies providing ship/waterside security services; and

.9 existing protective measures and procedures in effect, including inspection, control and monitoring equipment, personnel identification documents and communication, alarm, lighting, access control and other appropriate systems.

On-scene security survey

8.3 The company security officer should examine and evaluate existing shipboard protective measures, procedures and operations for:

.1 ensuring the performance of all ship security duties;

.2 monitoring restricted areas to ensure that only authorized persons have access;

.3 controlling access to the ship;

.4 monitoring of deck areas and areas surrounding the ship;

2. Throughout this Section references to the company security officer should allow for the duties to be performed by a ship security officer acting on behalf of the company security officer.

.5 controlling the embarkation of persons and their effects (luggage, baggage and crew's personal gear);

.6 supervising the handling of cargo and ship's stores; and

.7 ensuring that port-specific security communication, information, and equipment are readily available.

8.4 The company security officer should examine each identified point of access, including open weather decks, and evaluate its potential for use by individuals who might be engaged in unlawful acts. This includes individuals having legitimate access as well as those who seek to obtain unauthorized entry.

8.5 The company security officer should examine and evaluate existing protective measures, procedures and operations, under both emergency and routine conditions, including:

.1 established security guidance;

.2 response procedures to fire or other emergency conditions;

.3 the level of supervision of the ship's crew, vendors, repair technicians, dock workers, etc.;

.4 the frequency and effectiveness of security patrols;

.5 the security key-control and other access prevention systems;

.6 security communications systems and procedures; and

.7 security doors, barriers and lighting.

8.6 Key shipboard operations that are important to protect may include:

.1 cargo and ship stores operations;

.2 navigation; and

.3 passenger safety.

8.7 Possible threats to key ship board operations may include:

.1 bombing;

.2 sabotage;

.3 hijacking;

.4 unauthorized use;

.5 smuggling;

.6 cargo tampering;

.7 stowaways;

.8 vandalism; and

.9 transporting weapons of mass destruction.

8.8 Identification of weaknesses, including human factors in the infrastructure, may include:

.1 conflicting policies between safety and security measures;

.2 conflicting shipboard and security duty assignments;

.3 watchkeeping and manning constraints; and

.4 training deficiencies.

9 Ship Security Plan

General

9.1 Preparation of the Ship Security Plan (SSP) is the responsibility of the Company Security Officer (CSO). The content of each individual SSP should vary depending on the particular ship it covers. The Ship Security Assessment (SSA) will have identified the particular features of the ship, and the potential threats and weaknesses. The preparation of the SSP will require these features to be addressed in detail. Contracting States may prepare advice on the preparation and content of a SSP but all SSPs should:

.1 detail the security organisation of the ship, the ship's links with port facilities, other ships and relevant authorities and the necessary communication systems to allow the effective continuous operation of the ship and its links with others, including port facilities;

.2 detail the basic Security Level 1 measures, both operational and physical, that will be in place and the additional measures that will allow the ship to progress without delay to Security Level 2 and, when necessary, to Security Level 3, and

.3 provide for regular audit and review of the SSP and its amendment in response to experience or changing circumstances.

9.2 Preparation of an effective SSP will rest on a thorough assessment of all issues that relate to the security of the ship including, in particular, a thorough appreciation of the physical and operational characteristics of the individual ship.

9.3 All SSPs should be approved by the Company and the Administration. Company Security Officers should develop procedures to assess the continuing effectiveness of each SSP and amendment of the SSP subsequent to its approval.

9.4 The operational and physical measures included in the SSP should be in place within a reasonable period of the SSP's approval and the SSP should indicate when each measure will be in place. If there is likely to be any delay in their provision this should be discussed with the Company Security Officer responsible for approval of the SSP and satisfactory alternative

temporary security measures that provide an equivalent level of security should be agreed to cover any interim period.

Organisation and Performance of Ship Security Duties

9.5 The SSP should include the following which relate to all Security Levels:

.1 the organisational structure of security for the ship;

.2 the roles and responsibilities of all shipboard personnel with a security role and the performance measures needed to allow their individual effectiveness to be assessed;

.3 the command and reporting system for the ship's security and its links with port facilities and national or local authorities with security responsibilities;

.4 the communication systems provided to allow effective and continuous communication between shipboard personnel with a security role, port facilities, other ships and, when appropriate, with national or local authorities with security responsibilities;

.5 the procedures or safeguards necessary to allow such continuous communications to be maintained at all times;

.6 the procedures needed to assess the continuing effectiveness of security procedures and equipment, including procedures for identifying and responding to equipment failure or malfunction, and

.7 the procedures to allow the submission, and assessment, of reports relating to possible breaches of security or security concerns.

9.6 The remainder of this section looks specifically at the measures that could be taken at each Security Level covering:

.1 access to the Ship;

.2 restricted areas on the ship;

.3 embarkation of passengers and their effects;

.4 cargo and ship's stores, and

.5 monitoring the Ship.

Access to the Ship

9.7 The SSP should include protective measures covering the following means of access to the Ship:

.1 ladders;

.2 gangways;

.3 ramps;

.4 side ports;

.5 electronic information systems, and

.6 other access points identified in the SSA.

9.8 For each of these the SSP should identify the appropriate locations where access restrictions or prohibitions should be applied for each of the Security Levels. For each Security Level the SSP should specify the type of restriction or prohibition to be applied and the means of enforcing them.

9.9 Each SSP should indicate for each Security Level the means of identification required to allow access to the Ship and for individuals to remain on the ship without challenge.

9.10 Those unwilling or unable to establish their identity when requested to do so should be denied access to the ship and their attempt to obtain access should be reported to the Ship and Company Security Officers, and national or local authorities with security responsibilities.

9.11 The SSP should indicate separate locations for checked and unchecked persons and their effects.

9.12 The SSP should indicate the frequency of application of any access controls particularly if they are to be applied on a random, or occasional, basis.

Security Level 1

9.13 For Security Level 1 the SSP should establish protective measures to control access to the Ship, where the following may be applied:

.1 verification of the identity of passengers, crew, port facility staff and those employed within the port facility;

.2 for those not employed on the ship, restricting access only to those able to establish their identity;

.3 undertaking inspections of people, personal effects, vehicles and their contents to deter and detect the introduction of weapons, incendiaries and explosives on to the Ship;

.4 identification of access points that should be secured or continuously attended to prevent unauthorized access; and

.5 locking or taking precautions to prevent unauthorized access to weather-deck vents, storage lockers, and doors to normally unmanned spaces (such as storerooms, auxiliary machinery rooms, etc.).

Security Level 2

9.14 For Security Level 2 the SSP should establish measures to protect against a heightened risk of a security incident that may include:

.1 assign additional personnel to guard access points;

.2 limit the number of access points to the Ship, identify those to be closed and the means of adequately securing them;

.3 provide in co-ordination with a port facility, for the extension of access control to beyond the immediate area of the ship/port interface;

.4 increase the frequency of inspections of people, personal effects, vehicles and their contents to deter and detect the introduction of weapons, incendiaries and explosives on to the Ship;

Security Level 3

9.15 For Security Level 3, the SSP should establish measures to increase surveillance while significantly restricting access, to immediately identify and respond to security incidents. The measures are likely to be progressive and should consider as an alternative, changing ship/port interface locations to a port facility with a lower security level. However, appropriate Security Level 3 measures for consideration in the SSP could include:

.1 assigning additional personnel to guard access points and areas adjacent to access point; and

.2 limiting entry to the ship to a single access point;

.3 protecting electronic information systems.

Restricted Areas

9.16 The SSP should identify the restricted areas to be established on the ship, specify their extent, times of application, the measures to be taken to control access to them and those to be taken to control activities within them. The purpose of restricted areas are to:

.1 protect passengers, ship's personnel, and personnel from port facilities or other agencies authorised to be on board;

.2 protect key areas within the Ship, and

.3 protect cargo and ship's stores from interference.

9.17 The SSP should ensure that all restricted areas have clearly established policies and practices to control:

.1 access by individuals;

.2 the embarkation of passengers and their effects, and

.3 the loading and unloading of cargo and ship’s stores

9.18 The SSP should provide that all restricted areas should be clearly marked indicating that access to the area is restricted and that unauthorised presence within the area constitutes a breach of security.

9.19 Restricted areas can include:

.1 navigational bridge;

.2 control station and control stations as defined in Chapter11-2 of the Convention;

.3 machinery spaces of category A as defined in Chapter 11-2 of the Convention;

.4 machinery spaces containing propulsion machinery, generators and major electrical machinery, main and auxiliary steering gear, ventilation and air-conditioning machinery and similar spaces;

.5 spaces with access to potable water tanks, pumps, or manifolds;

.6 cargo pump room; and

.7 any other areas as determined by the Company Security Officer to which access must be restricted to maintain the security of the ship.

Security Level 1

9.20 At Security Level 1 operational and physical measures applying to restricted areas can include:

.1 locking or securing access points;

.2 using surveillance equipment, such as closed circuit television (CCTV);

.3 using personnel as security guards or patrols; and

.4 using automatic intrusion detection devices to alert the crew of unauthorized access to restricted areas. When used, automatic intrusion detection devices should activate an audible and/or visual alarm; and indicate in a location that is continuously manned or monitored.

Security Level 2

9.21 At Security Level 2 the frequency and intensity of the monitoring of, and control of access to restricted areas should be increased to ensure that only authorized persons have access. Measures could include:

.1 securing additional access points and areas adjacent to access points;

.2 continuously monitoring surveillance equipment, such as closed circuit television (CCTV);

.3 dedicating personnel to guarding and patrolling restricted areas; and

.4 using additional automatic intrusion detection devices on areas adjacent to restricted areas.

Security Level 3

9.22 For Security Level 3, the SSP should establish measures to increase surveillance while significantly restricting access to the restricted area, to immediately identify and respond to security incidents. Additional measures applying to restricted areas at Security Level 3 could include:

.1 securing all access points and areas adjacent to access points;

.2 posting personnel to continuously guard all restricted areas; and

.3 assigning personnel to continuously patrol restricted areas and areas adjacent to restricted areas.

Embarkation of Persons and their Effects

9.23 It is important to control the embarkation of persons and their effects to adequately identify and take preventive measures against security incidents.

Security Level 1

9.24 At Security Level 1 the following measures could be taken:

.1 verifying reason personnel are embarking the ship by using tickets, boarding passes, work orders or other means;

.2 inspecting persons, baggage, carry-on items, and personal gear for prohibited weapons, incendiaries, and explosives; and

.3 positively identifying crewmembers prior to boarding and verifying them as authorized to serve aboard the ship.

9.25 Areas should be designated to check baggage, carry-on items, and personal gear. Access to and from these areas should be controlled to segregate checked persons and articles from unchecked persons and articles.

Security Level 2

9.26 At Security Level 2 measures could be enhanced to include:

.1 increasing the frequency and detail of inspecting persons, baggage, carry-on items and personal gear entering the ship for prohibited weapons, incendiaries, and explosives;

.2 assigning personnel to guard designated areas; and

.3 positively identifying passengers, visitors, and other personnel prior to each embarkation.

9.27 Security briefings should be provided to all crew and passengers, prior to departing, on any specific threats and the need for vigilance and reporting suspicious persons, objects, or activities.

Security Level 3

9.28 At Security Level 3, the SSP should establish measures to increase the detail and frequency of controls used on persons embarking as well as their effects, to immediately identify and respond to security incidents. Specific measures should, for example, include:

.1 inspecting all persons, baggage, carry-on items and crewmembers personal gear for prohibited weapons, incendiaries, and explosives;

.2 limiting entry only to passengers and crewmembers;

.3 escort all service providers or other personnel needed aboard to provide essential services to the ship;

.4 assigning additional personnel to guard designated areas; and

.5 assigning personnel to continuously patrol designated areas.

9.29 Security briefings should be provided to all crew and passengers, prior to each embarkation and disembarkation, on any specific threats and the need for vigilance and reporting suspicious persons, objects, or activities.

Cargo and Ship's Stores

9.30 Cargo and ship's stores needs to be controlled to:

.1 prevent tampering, and

.2 prevent unauthorised cargo and ship's stores from being accepted and stored on board the ship.

9.31 Control measures will involve inventory control procedures at access points to the ship. Once on board the Ship, cargo and ship's stores should be capable of being identified as having been approved for loading on to the ship or into a restricted area and procedures and practices should be applied to ensure that cargo and stores are not tampered with once on board.

Security Level 1

9.32 At Security Level 1 the following measures could be taken:

.1 verifying cargo and ship's stores against the manifest;

.2 verifying the integrity of cargo and ship's stores to ensure that they have not been tampered with; and

.3 inspecting vehicles on passenger ships.

9.33 Verification and checking of cargo and ship's stores may be accomplished by:

.1 visual and physical examination;

.2 using scanning/detection equipment, mechanical devices, or canines; and

.3 coordinating with the shipper or other responsible party through an established agreement and procedures.

Security Level 2

9.34 At Security Level 2 the frequency and detail of the inventory control and inspection regime could be enhanced to include:

.1 verifying cargo and ship's stores against the manifest;

.2 verifying integrity of cargo and ship's stores to ensure that they have not been tampered with; and

.3 inspecting vehicles on passenger ships.

9.35 Increased verification and checking of cargo and ship's stores may be accomplished by:

.1 increasing the frequency and detail of visual and physical examination;

.2 increasing the frequency of the use of scanning/detection equipment, mechanical devices, or canines; and

.3 coordinating enhanced protective measures with the shipper or other responsible party in addition to an established agreement and procedures.

Security Level 3

9.36 At Security Level 3, the SSP should establish measures to increase supervision of cargo and ship's stores, to immediately identify and respond to security incidents. The requirements for Security Level 3 should, for example, include:

.1 verifying all cargo and ship's stores against the manifest;

.2 verifying integrity of all cargo and ship's stores to ensure that they have not been tampered with; and

.3 inspecting all vehicles on passenger ships.

9.37 Verification and checking of cargo and ship's stores may be accomplished by:

.1 continually conducting visual and physical examinations;

.2 continually using scanning/detection equipment, mechanical devices, or canines; and

.3 coordinating enhanced protective measures with the shipper or other responsible party in addition to an established agreement and procedures.

Monitoring the Ship

9.38 The Ship should have the capability to monitor the Ship and areas surrounding the ship at all times, and in all conditions. Such monitoring can include use of:

.1 lighting;

.2 guards, including patrols, and

.3 automatic alarms and surveillance equipment, including CCTV.

9.39 The SSP should specify the procedures and equipment needed at each Security Level and the means of ensuring that monitoring is continuous, including consideration of the possible effects of power disruptions.

Security Level 1

9.40 At security Level 1, a combination of lighting, security guards and surveillance equipment should allow ship security personnel to observe the ship in general, and barriers and restricted areas in particular.

9.41 The Ship's deck and access points to the ship should be illuminated while conducting ship/port interface activities. While underway, ships should use the maximum lighting available consistent with safe navigation, having regard to the provisions of the 1972 COLREGS. A ship should consider the following in establishing the appropriate level and location of lighting:

.1 crewmembers should be able to see beyond the ship, both pier side and waterside; and

.2 coverage should include the area on and around the ship;

.3 coverage should facilitate personnel identification at access points; and

.4 coverage may be provided through coordination with the port facility.

Security Level 2

9.42 At Security Level 2 monitoring and surveillance could be enhanced by:

.1 increasing the frequency and detail of security patrols;

.2 increasing the use of security equipment;

.3 assigning additional personnel as security lookouts; and

.4 coordinating waterside boat patrols with the port facility.

9.43 Additional lighting may be necessary to protect against a heightened risk of a security incidents. When necessary, additional lighting may be accomplished by coordinating with the port facility to provide additional shore side lighting.

Security Level 3

9.44 At Security Level 3, the SSP should establish measures to increase monitoring of the ship, to immediately identify and respond to security incidents. However, additional measures should, for example, include:

.1 increasing the number and frequency of security patrols to ensure continuous monitoring; and

.2 increasing the number and frequency of waterside boat patrols with the port facility to ensure continuous monitoring.

9.45 Additional lighting necessary to immediately identify and take preventive measures against security incidents may be accomplished by:

.1 using spotlights and floodlights to enhance visibility of the deck and areas surrounding the ship;

.2 using lighting to enhance visibility of the surrounding water and waterline; and

.3 using divers to inspect the underwater pier structures prior to the ship's arrival, upon the ship's arrival, and in other cases deemed necessary.

Differing Security Levels

9.46 The SSP should include details of the approach the Ship will adopt if a port facility being used is at a lower Security Level than that applying to the Ship.

Declarations of Security

9.47 The SSP should detail when the Ship Security Officer will request a Declaration of Security and how requests for Declarations of Security from a port facility will be handled.

Audit and Review

9.48 The SSP should indicate how the Company Security Officer intends to audit the continued effectiveness of the SSP and the procedure to be followed to review, update or amend the SSP.

Contact Point

9.49 The SSP should include the details of the contact point, which can be published, for the Company Security Officer.

10 Records

No additional guidance.

11 Company Security Officer

No additional guidance.

12 Ship Security Officer

No additional guidance.

13 Training and Drills

13.1 The Company Security Officer and appropriate shore based personnel should have knowledge of and receive training in accordance with Part A of this Code in some or all of the following, as appropriate:

.1 security administration;

.2 relevant international conventions, codes and recommendations;

.3 responsibilities and functions of other involved organisations;

.4 relevant government legislation and regulations;

.5 methodology of a security assessment;

.6 security surveys and inspections;

.7 ship and port facility security measures;

.8 security training and education;

.9 recognition of characteristics and behavioural patterns of persons who are likely to threaten the security of the ship;

.10 inspection, control and monitoring techniques;

.11 techniques used by others to circumvent protective measures;

.12 recognition and detection of weapons, dangerous substances and devices;

.13 ship and local port operations and conditions;

.14 security devices and systems; and

.15 methods of physical searches and non-intrusive inspections.

13.2 The Ship Security Officer should have adequate knowledge of and receive training in accordance with Part A of this Code in some or all of the following, as appropriate:

.1 the ship security plan and related procedures (including scenario-based training on how to respond);

.2 the layout of the ship;

.3 methodology of a security assessment;

.4 methods of conducting security inspections;

.5 techniques used by others to circumvent protective measures;

.6 operation of technical aids for security, if used;

.7 recognition of characteristics and behavioural patterns of persons who are likely to threaten the security of the ship;

.8 recognition and detection of weapons, dangerous substances and devices;

.9 port and ship operations;

.10 methods of physical searches and non-intrusive inspections; and

.11 instruction techniques for training crewmembers on security procedures and duties.

13.3 Shipboard personnel having specific security duties should all know their responsibilities for ship security as described in the Ship Security Plan and should all have sufficient knowledge and ability to perform their assigned duties, including:

.1 inspection, control, and monitoring duties required by pertinent regulations, policies, and laws;

.2 detection and identification of weapons, and other dangerous substances and devices;

.3 operation, calibration, underway maintenance, and testing of security equipment;

.4 physical search methods of persons, baggage, cargo, and vessel stores;

.5 emergency procedures;

.6 recognition of characteristics and behavioural patterns of persons who are likely to threaten the security of the ship;

.7 techniques that foster calming behaviour; and

.8 techniques used by others to circumvent protective measures.

13.4 Ships should conduct detailed drills at least monthly or more frequently, as necessary, to ensure that crewmembers are proficient in all assigned security duties for all security levels.

14 Port Facility Security

Additional guidance on port facility security is given in Section 15 on the Port Facility Security Assessment and Section 16 on the Port Facility Security Plan.

15 Port Facility Security Assessment

15.1 Contracting Governments should decide if additional requirements are necessary to complete a Port Facility Security Assessment. Contracting Governments should communicate any such additional requirements to their trading partners.

15.2 Contracting Governments should not delegate responsibility for approval of a port facility security assessment.

15.3 If a Contracting Government uses a non-governmental organisation to review and verify compliance of the port facility security assessment, such an organisation should not be associated with any other non-governmental organisation that prepared or assisted in the preparation of that assessment.

15.4 A port facility security assessment should address the following elements within a port facility:

.1 physical security;

.2 structural integrity;

.3 personnel protection systems;

.4 procedural policies;

.5 communication systems;

.6 electronic systems:

.7 transportation infrastructure;

.8 utilities; and,

.9 other areas that may, if damaged, pose a risk to people, property, or operations.

15.5 The port facility security assessment should be carried out by competent persons, who have been properly vetted for trustworthiness by the Contracting Government, with the skills to evaluate the security of a port facility. Such persons should be skilled in, or able to draw upon expert assistance in relation to:

.1 methods used to cause a security incident;

.2 effects of explosives on structures and port facility service suppliers;

.3 port facility security;

.4 port business practices;

.5 emergency preparedness;

.6 physical security;

.7 communications;

.8 civil engineering;

.9 ship and port operations; and,

.10 contingency planning.

Identification and evaluation of important assets and infrastructure it is important to protect

15.6 The identification and evaluation of important assets and infrastructure is a process through which the relative importance of structures and installations to the functioning of the port facility can be established. This identification and evaluation process is important because it provides a basis for focusing mitigation strategies on those assets and structures which it is more important to protect from a security incident. This process should take into account potential loss of life, areas of public accommodation, the economic significance of the port, symbolic value, and the presence of government installations.

15.7 Identification and evaluation of assets and infrastructure should be used to prioritise their relative importance for protection. The primary concern should be whether the port facility, structure or installation can continue to function without the asset, and the extent to which rapid reinstatement of normal functioning is possible.

15.8 Assets and infrastructure that may be included are:

.1 facilities, terminals, storage areas, and cargo handling equipment;

.2 systems such as computer data systems, electrical distribution systems, and communication systems;

.3 power plants, cargo transfer piping, and water supplies;

.4 bridges, railways, roads; and

.5 structures adjacent to the port facility.

15.9 The clear identification of assets and infrastructure is essential to the evaluation of the port facility, the prioritisation of protective measures, and decisions concerning the allocation of resources to better protect the port facility.

Identification of the possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritise security measures

15.10 Possible acts that could threaten the security of assets and infrastructure, and the methods of carrying out those acts, should be identified to evaluate the vulnerability of a given asset or location to a security incident, and to establish and prioritise security-program requirements, planning, and resource allocations. Identification and evaluation of each potential act and its method should be based on various factors, including threat assessments by government agencies. By identifying and assessing threats, organisations do not have to rely on worst-case scenarios to guide planning and resource allocations.

15.11 Identification of possible acts that could threaten the security of assets and infrastructure and the likelihood of their occurrence, should include:

.1 analysis of the possible threats in terms of capability, intention, and feasibility;

.2 analysis of the consequences of the threat; and

.3 the likelihood of the threat occurring.

15.12 Security incidents affecting assets and infrastructure may include:

.1 bombing of facilities, terminals, storage areas, and sabotage of cargo handling equipment;

.2 sabotage or unauthorised use of systems such as computer data systems, electrical distribution systems, and communication systems;

.3 vandalism or sabotage of power plants, cargo transfer piping, and water supplies;

.4 destruction of bridges, railways, roads;

.5 destruction of or smuggling from adjacent structures to the port facility; and

.6 chemical, biological and radiological attack.

Identification, selection, and prioritisation of countermeasures and procedural changes and their level of effectiveness in reducing vulnerability

15.13 The identification and prioritization of countermeasures is designed to ensure that the most effective countermeasures are used to reduce the vulnerability of a port facility or ship/port interface to the possible threats. Countermeasures and procedural changes should be selected on the basis of factors such as whether they reduce the probability of an undesired event occurring and any additional enforcement or audit requirements.

15.14 Countermeasures should be evaluated using information that includes:

.1 security surveys;

.2 discussions with key asset owners/operators;

.3 historical information on security incidents; and

.4 operations within the port facility.

Identification of weaknesses, including human factors in the infrastructure, policies and procedures

15.15 Identification of weaknesses in physical structures, personnel protection systems, processes, or other areas that may lead to a security incident can be used to establish options to eliminate or mitigate those weaknesses. For example, an analysis might reveal weaknesses in an organisation's security systems or unprotected key infrastructure such as water supplies, bridges, and tunnels that could be resolved through physical enhancements.

15.16 Identification of weaknesses, including human factors in the infrastructure, policies, and procedures should include:

.1 structural integrity of the piers, facilities, and associated structures;

.2 protection systems used for employees and security personnel;

.3 existing security procedures and communications;

.4 communication equipment capabilities;

.5 port services and utilities;

.6 other areas that may be exploited;

.7 existing security measures;

.8 existing agreements with private security companies providing land/waterside security services;

.9 conflicting policies between safety and security measures;

.10 conflicting port facility and security duty assignments;

.11 enforcement and manning constraints; and

.12 training deficiencies.

16 Port Facility Security Plan

General

16.1 Preparation of the Port Facility Security Plan (PFSP) is the responsibility of the Port Facility Security Officer (PFSO). The content of each individual PFSP should vary depending on the particular circumstances of the Port Facility, or Facilities, it covers. The Port Facility Security Assessment will have identified the particular features of the port, and of the potential threats, that have led to the need to appoint a PFSO and to prepare a PFSP. The preparation of the PFSP will require these features, and other local or national security considerations, to be addressed in detail. Contracting States may prepare advice on the preparation and content of PFSP but all PFSPs should:

.1 detail the security organisation of the Port Facility, the organisation's links with other relevant authorities and the necessary communication systems to allow the effective continuous operation of the organisation and its links with others, including ships in port;

.2 detail the basic Security Level 1 measures, both operational and physical, that will be in place and the additional measures that will allow the Port Facility to progress without delay to Security Level 2 and, when necessary, to Security Level 3, and

.3 provide for regular audit and review of the PFSP and its amendment in response to experience or changing circumstances.

16.2 Preparation of an effective PFSP will rest on a thorough assessment of all issues that that relate to the security of the Port Facility including, in particular, a thorough appreciation of the physical and operational characteristics of the individual Port Facility.

16.3 All PFSPs should be approved by the Contracting Government in whose area, or jurisdiction, the Port Facility is situated. Contracting Governments should develop procedures to assess the continuing effectiveness of each PFSP and may require amendment of the PFSP prior to its initial approval or subsequent to its approval. The FSPS should make provision for the

retention of records of audits, training, drills and exercises as evidence of compliance with those requirements.

16.4 The operational and physical measures included in the PFSP should be in place within a reasonable period of the PFSP's approval and the PFSP should indicate when each measure will be in place. If there is likely to be any delay in their provision this should be discussed with the Contracting Government responsible for approval of the PFSP and satisfactory alternative temporary security measures that provide an equivalent level of security should be agreed to cover any interim period.

16.5 Contracting Governments should also consider the control and communication methods used for ships and other craft transiting in or near port facilities and not subject to this Code. Recreational or other water traffic may be impacted by security level measures and should be controlled to ensure the ship/port interface remains secure.

Organisation and Performance of Port Facility Security Duties

16.6 The PFSP should include the following which relate to all Security Levels:

.1 the organisation of the port facility security organisation;

.2 the roles and responsibilities of all port facility personnel with a security role and the performance measures needed to allow their individual effectiveness to be assessed;

.3 the command and reporting system of the port facility security organisation and its links with other national or local authorities with security responsibilities;

.4 the communication systems provided to allow effective and continuous communication between port facility security personnel, ships in port and, when appropriate, with national or local authorities with security responsibilities;

.5 the procedures or safeguards necessary to allow such continuous communications to be maintained at all times;

.6 the procedures needed to assess the continuing effectiveness of security procedures and equipment, including procedures for identifying and responding to equipment failure or malfunction, and

.7 the procedures to allow the submission, and assessment, of reports relating to possible breaches of security or security concerns.

16.7 The remainder of this section looks specifically at the measures that could be taken at each Security Level covering:

.1 Access to the Port Facility;

.2 Restricted areas within the Port Facility;

.3 Cargo and ship's stores, and

.4 Monitoring the Port Facility.

Access to the Port Facility

16.8 The PFSP should include protective measures covering the following means of access to, and locations allowing observation of, the Port Facility:

.1 waterways, including approaches, ship manoeuvering areas, rivers and canals;

.2 roadways;

.3 walkways;

.4 rail lines;

.5 piers;

.6 adjacent structures or locations which allow observation of all, or part, of the Port Facility, and

.7 electronic information systems.

16.9 For each of these the PFSP should identify the appropriate locations where access restrictions or prohibitions should be applied for each of the Security Levels. For each Security Level the PFSP should specify the type of restriction or prohibition to be applied and the means of enforcing them.

16.10 Each PFSP should indicate for each Security Level the means of identification required to allow access to the Port Facility and for individuals to remain within the Port Facility without challenge.

16.11 Those unwilling or unable to establish their identity when requested to do so should be denied access to the Port Facility and their attempt to obtain access should be reported to the national or local authorities with security responsibilities.

16.12 The PFSP should identify the locations where people, personal effects, and vehicle inspections are to be undertaken.

16.13 The PFSP should indicate separate locations for checked and unchecked persons and their effects.

16.14 The PFSP should indicate the frequency of application of any access controls particularly if they are to be applied on a random, or occasional, basis.

Security Level 1

16.15 For Security Level 1 the PFSP should establish control points where the following may be applied:

.1 verification of the identity of Port Facility staff and those employed within the Port Facility and their vehicles;

.2 for those not employed within the Port Facility restricting access to individuals or their vehicles only to those able to establish their identity;

.3 undertaking inspections of people, personal effects, vehicles and their contents to deter and detect the introduction of weapons, incendiaries and explosives into the Port Facility; and

.4 identification of any access points not in regular use which should be permanently closed and locked.

Security Level 2

16.16 For Security Level 2 the PFSP should:

.1 assign additional personnel to guard access points and perimeter barriers;

.2 limit the number of access points to the Port Facility, identify those to be closed and the means of adequately securing them;

.3 provide for means of impeding movement through the remaining access points, e.g. security barriers;

.4 increase the frequency of people, personal effects, and vehicle inspection;

.5 deny access to visitors who are unable to provide a verifiable justification for seeking access to the Port Facility.

Security Level 3

16.17 The security measures to apply in respect of Security Level 3 will be set by the Contracting Government responsible for the Port Facility. The measures are likely to be progressive and could include a complete bar on access to the Port Facility. However, appropriate Security Level 3 measures for consideration in the PFSP could include:

.1 further limiting the number of access points to the Port Facility and enhancing the level of security at such access points and in their immediate vicinity;

.2 establishing an enhanced security presence at all closed access points;

.3 further restricting access by individuals or vehicles and requiring those allowed access who are not Port Security Personnel to be escorted;

.4 inspecting all people, personal effects, and vehicles entering the Port Facility;

.5 taking measures, in conjunction with other security organisation, to limit or control access to buildings or locations from which the Port Facility can be overlooked or observed, and

.6 protecting electronic information systems.

<u>Restricted Areas</u>

16.18 The PFSP should identify the restricted areas to be established within, or immediately adjoining, the Port Facility, specify their extent, times of application, the measures to be taken to control access to them and those to be taken to control activities within them. The purpose of restricted areas are to:

.1 protect passengers, crews and Port Facility personnel;

.2 protect vessels using the Port Facility;

.3 protect key areas within the Port Facility, and

.4 protect cargo and ship stores from interference.

16.19 The PFSP should ensure that all restricted areas have clearly established policies and practices to control:

.1 access by individuals;

.2 the entry, parking, loading and unloading of vehicles;

.3 movement and storage of cargo and ship's stores, and

.4 unattended passenger effects.

16.20 The PFSP should provide that all restricted areas should be clearly marked indicating that access to the area is restricted and that unauthorised presence within the area constitutes a breach of security. When automatic alarm systems are employed they should alert a control centre which can respond to the triggering of an alarm.

16.21 Restricted areas can include:

.1 shore and waterside areas immediately adjacent to the ship;

.2 passenger and crew processing and embarkation areas;

.3 areas where loading or unloading of ships' cargo and stores is undertaken;

.4 locations where cargo manifest, or other security sensitive information, is held;

.5 port control buildings and facilities;

.6 essential electrical, water and other utility installations, and

.7 other locations in, or adjacent to, the Port Facility where access by vessels, vehicles and individuals should be restricted.

Security Level 1

16.22 At Security Level 1 operational and physical measures applying to restricted areas can include:

.1 provision of permanent or temporary barriers to surround the restricted area;

.2 provision of access points where access can be controlled by security guards when in operation and which can be effectively locked or barred when not in use;

.3 providing passes which must be displayed to identify individuals entitlement to be within the restricted area;

.4 clearly marking vehicles, cargo, or ship store's as approved for entry to the restricted area;

.5 provide patrols, automatic alarm systems, or surveillance equipment to detect unauthorised access into, or movement within, restricted areas, and

.6 restrictions on the movement of unauthorised craft in the vicinity of ships using the port facility.

Security Level 2

16.23 At Security Level 2 the frequency and intensity of the monitoring of, and control of access to, restricted areas should be increased. Measures could include:

.1 enhancing the effectiveness of the barriers or fencing surrounding restricted areas, including the use of foot patrols or automatic alarm systems;

.2 reducing the number of access points to restricted areas and enhancing the controls applied at the remaining accesses;

.3 further restricting access to the restrict areas and movements and storage within them;

.4 use of continuously monitoring surveillance equipment, such as closed circuit television (CCTV);

.5 enhancing the number and frequency of patrols undertaken on the boundaries of the restricted areas and within the areas;

.6 restricting access to areas adjacent to the restricted areas; and

.7 enforcing restrictions on access by unauthorised craft to the waters adjacent to ships using the Port Facility.

Security Level 3

16.24 Specific measures should be defined for application at Security Level 3 by the Contracting Government responsible for the Port Facility. Additional measures applying to restricted areas at Security Level 3 could include:

.1 prohibiting access to restricted areas except for Port Facility Security and essential safety personnel;

.2 maintaining permanent foot patrols on, or adjacent to, the perimeters of the restricted areas;

.3 clearing restricted areas of non-essential personnel, vehicles, cargo or ship's stores;

.4 further enhancing CCTV coverage and the use of automatic alarms;

.5 establishing teams to search restricted areas, and

.6 providing boat patrols to control access to the waters adjacent to ships using the Port Facilities.

Cargo and Ship's Stores

16.25 Cargo and ship's stores needs to be controlled to:

.1 prevent tampering, and

.2 prevent unauthorised cargo and ship's stores from being accepted and stored within the Port Facility.

16.26 Control measures will involve inventory control procedures at access points to the Port Facility. Once within the Port Facility cargo and ship's stores should be capable of being identified as having been approved for entry to the Port Facility or a restricted area and procedures and practices should be applied to ensure that cargo and stores have not been interfered with once within the Port Facility.

Security Level 1

16.27 At Security Level 1 the following measures could be taken:

.1 inventory control

.2 visual and physical inspection;

.3 development of a movement and storage plan, including identification of secure storage areas;

.4 use of scanning equipment, mechanical devices, or canines, and

.5 developing agreements with cargo and stores handlers on the procedures to be followed at the particular Port Facility.

Security Level 2

16.28 At Security Level 2 the inventory control and inspection regime could be enhanced to:

.1 increase the frequency and intensity of visual and physical examinations;

.2 review the movement and storage plans to restrict the movement of cargo and ship's stores with the Port Facility and to limit the number of secure locations where they could be stored;

.3 restrict, or prohibit, entry of cargo and ship's stores connected to ships that will not leave the Port Facility within a specified period;

.4 increase the frequency of inventory inspections;

.5 increase the use of scanning equipment and other search methods;

.6 agree to variations to any agreements with cargo and stores handlers to provide an appropriate response to the increased Security Level.

Security Level 3

16.29 The requirements for Security Level 3 will be established by the Contracting Government but could include:

.1 further restricting entry and storage of cargo and ship's stores only to those essential to operations;

.2 further increasing the frequency of inventory inspections and physical searches;

.3 limiting the locations where cargo and ship's stores can be stored, including prohibiting storage in close proximity to ships or essential Port Facility installations, and

.4 arranging temporary storage or screening facilities outside the Port Facility.

Monitoring the Port Facility

16.30 The Port Facility should have the capability to monitor the Port Facilities and the approaches, on land and water, at all times, including the night hours and periods of limited visibility. Such monitoring can include use of:

.1 lighting;

.2 guards, including foot, vehicle and waterborne patrols, and

.3 automatic alarms and surveillance equipment, including CCTV.

16.31 The PFSP should specify the procedures and equipment needed at each Security Level and the means of ensuring that monitoring equipment will be able to perform continually, including consideration of the possible effects of power disruptions.

Security Level 1

16.32 At Security Level 1 a combination of lighting, security guards and surveillance equipment should allow port facility security personnel to:

.1 observe the general Port Facility Area, including land and water-side accesses to it;

.2 observe access points, barriers and restricted areas, and

.3 allow port facility security personnel to monitor areas and movements adjacent to ships using the Port Facility, including augmentation of lighting provided by the ship itself.

Security Level 2

16.33 At Security Level 2 monitoring and surveillance could be enhanced by:

.1 increasing the coverage and intensity of lighting and surveillance equipment, including the provision of additional lighting and CCTV coverage;

.2 increasing the frequency of foot, vehicle or waterborne patrols, and

.3 assigning additional security personnel to monitor and patrol.

Security Level 3

16.34 The specific requirements relating to Security Level 3 will be set by the Contracting Government having responsibility for the Port Facility. However, additional measures could include:

.1 further intensification of lighting and the coverage of surveillance equipment;

.2 further increases in the frequency of patrols including patrols in the vicinity of the Port Facility and the use of other security personnel to reinforce port security personnel, and

.3 use of divers to inspect piers and vessels.

Differing Security Levels

16.35 The PFSP could include details of the approach the Port Facility will adopt if a ship using the Port facility is at a higher Security Level than that applying to the Port Facility.

Declarations of Security

16.36 The PFSP should detail when the Port Facility Security Officer will request a Declaration of Security and how requests for Declarations of Security from a ship will be handled.

Audit and Review

16.37 The PFSP should indicate how the Port Facility Security Officer intends to audit the continued effectiveness of the PFSP and the procedure to be followed to review, update or amend the PFSP.

Contact Point

16.38 The PFSP should include the details of the contact point, which can be published, for the Port Facility Security Officer.

Approval of Port Security Plans

16.39 Port Security Plans have to be approved by the relevant Contracting Government and Contracting Governments should establish appropriate procedures to provide for:

.1 the submission of PFSPs to them;

.2 the consideration of PFSPs;

.3 the approval of PFSPs, with or without amendments;

.4 consideration of amendments submitted after approval, and

.5 procedures for inspecting or auditing the continuing relevance of the approved PFSP.

17 Port Facility Security Officer

No additional guidance.

18 Training and Drills

18.1 The Port Facility Security Officer and appropriate port facility security personnel should have knowledge and receive training in some or all of the following, as appropriate:

.1 security administration;

.2 relevant international conventions, codes and recommendations;

.3 responsibilities and functions of other involved organisations;

.4 relevant government legislation and regulations;

.5 risk, threat and vulnerability assessments;

.6 security surveys and inspections;

.7 ship and port facility protective measures;

.8 security training and education;

.9 recognition of characteristics and behavioural patterns of persons who are likely to threaten the security of the port facility;

.10 inspection, control and monitoring techniques;

.11 techniques used to circumvent protective measures;

.12 recognition and detection or weapons, dangerous substances and devices;

.13 ship and local port operations and conditions;

.14 security devices and systems; and

.15 methods of physical searches and non-intrusive inspections.

18.2 Port facility should conduct frequent and detailed drills to ensure that port facility personnel are proficient in all assigned security duties for all security levels.

ANNEX

Declaration of Security

_____ _____
(Name of Port Facility) (Name of Ship)

This Declaration of Security is valid from _____ until _____, for the following ship/port interface activities under Security Level ____:

_____

_____

The port facility and ship agree to the following security responsibilities to ensure compliance with the requirement in the International Ship and Port Facility Security Code.

Activity	The Port Facility will: (*briefly describe arrangements)*	The Ship will: (*briefly describe arrangements)*
1. Ensuring the performance of all security duties		
2. Monitoring restricted areas to ensure that only authorized personnel have access		
3. Controlling access to the port facility and ship		
4. Monitoring of port facility and ship, including mooring areas and areas surrounding the ship		
5. Supervising the handling of cargo and ship stores		
6. Controlling the embarkation of persons and their effects		
7. Ensuring that security communication is readily available between the ship and port facility		

The signatories to this agreement certify that security arrangements for both the port facility and the ship during the specified ship/port interface activities meet the provisions of the Code.

Date of issue ……

_____
(Signature of Port Facility Security Officer or authorized designee)
Name and Title of Port Facility Security Officer:

_____
Contact arrangements_____

_____
Mailing Address:

_____
(Signature of Master or Ship Security Officer)

Name and Title of Ship Security Officer:
_____
Contact arrangements_____

_____
Particulars of the ship:
Registry_____
IMO number:_____